In the claims:

1. (currently amended) A method of securing packet data transferred between a pair of stations of a group of more than two stations [[over]] on a backbone, the backbone comprising an ingress point and egress point, the method comprising the steps of:

~~receiving, at the ingress point of the backbone, group security association data associated with the group of stations;~~

receiving a packet at the ingress point of the backbone from any sending station of the group of stations, the [[a]] packet including an original header with a source IP address of the sending station and a destination IP address of a receiving station of the group of stations;

transforming, at the ingress point of the backbone, the packet by adding a group header including a group identifier corresponding to the group of stations and a destination address for the packet;

transforming, at the ingress point of the backbone, the packet according to the group security association associated with the group identifier, wherein the ingress point is a provider edge device; [[and]]

forwarding the transformed packet over the backbone to the egress point using the group identifier as a backbone address;

receiving, at the egress point in the backbone, the transformed packet;

restoring, at the egress point in the backbone, the transformed packet according to the group security association associated with the group identifier;

transforming, at the egress point in the backbone, the restored packet by removing the group header; and

forwarding the restored transformed packet to the receiving station,

whereby the same security association is used for communications between any pair of stations of the group of stations.

2. (currently amended) The method according to claim 1, wherein the step of transforming at the ingress point of the backbone includes the step of retaining fields of the packet needed to transfer the packet to the destination address of the receiving station from the egress point ~~over the backbone~~.

3. (cancelled)

4. (cancelled)

5. (cancelled)

6. (cancelled)

7. (cancelled)

8. (cancelled)

9. (cancelled)

10. (currently amended) A network architecture for providing secure point-to-point communication between at least two members of a private network including more than two members over a communication link, the network architecture comprising:

a first station which is any one of the more than two members of the private network;

an ingress point to the communication link~~, wherein the communication link comprises a plurality of provider devices, and wherein the ingress point is one of the plurality of provider devices~~;

an egress point from the communication link;

a second station, coupled to the egress point;

the ingress point functioning to:

receive a packet from the first station, the packet including an original header with a source IP address of the first station and a destination IP address of the second station;

transform the packet by adding a group header including a group identifier corresponding to the group of stations and a destination address for the packet;

transform the packet according to the group security association associated with the group identifier; and

forward the transformed packet over the backbone to the egress point using the group identifier as a backbone address;

the egress point functioning to:

receive the transformed packet;

restore the transformed packet according to the group security association associated with the group identifier;

transform the restored packet by removing the group header; and

forward the restored transformed packet to the receiving station,

whereby the same security association is used for communications between any pair of stations of the group of stations

~~a group security association, corresponding to a group of stations in a private network, both the first station and the second station being members of the group and wherein a group identifier is associated with the group;~~

~~means for securing data transferred between members of the group from the ingress point and the egress point in the network using the group security association by transforming the data at the ingress point using a group security association associated with the group identifier;~~

~~means for forwarding the communication between members of the group over the network using a group address associated with the group, the group address including the group identifier and a group destination address.~~

11. (cancelled)

12. (original) The network architecture of claim 10, wherein the communication link comprises a plurality of provider devices, and wherein the egress point is one of the plurality of provider devices.

13. (original) The network architecture of claim 10, wherein the group comprises at least three stations.

14. (cancelled)

15. (cancelled)

16. (original) The network architecture according to claim 10 wherein the means for securing data includes transform logic for encrypting only a portion of data transferred between the ingress point and egress point of the communication link.